Protocole I.P. : réseaux et sous-réseaux (locaux)

Sur la toile, I.P. sert à la mise en relation des serveurs entre eux. Toute machine devant se connecter à l´Internet doit posséder une couche TCP/IP qui lui permettra le surf de page en page sur la toile. Si cette machine fait partie d´un réseau local (entreprise, administration ou plus simplement réseau familial), la même couche réseau TCP/IP peut servir de protocole pour ce réseau local.

Pourquoi des sous-réseaux ?

Dans un réseau comportant un grand nombre de machine, il devient nécessaire de subdiviser l´ensemble pour optimiser les échanges entre les machines.

Une **segmentation physique** par est certainement la solution la plus radicale car elle s'opère au niveau des couches 2 et 3 (couche de liaison physique et couche réseau) ; on constitue des réseaux virtuels en programmant des commutateurs ("*switch*") administrables: Cette tâche supplémentaire dans la gestion d´un réseau est délicate de par sa rigidité ; elle exige un plan physique de l´utilisation de chacune des prises réseau de l´entreprise et toute modification, aussi petite soit-elle, doit être répercutée sur tous les commutateurs.
Sachant que la couche 4 de transport doit de toutes façons être gérée (par le protocole TCP/IP), il peut se concevoir de subdiviser le réseau global en utilisant une **segmentation logique** grâce au même protocole de transport. Cette méthode s' appelle le '*subnetting*' ou la création de sous-réseaux. Elle permet d'éviter une dégradation de la bande passante quand trop de machines sont sur le même réseau. Si des routeurs (ils appartiennent à la couche 3) sont utilisés, le trafic de diffusion des trames ("*broadcast*") sera limité à chacun des sous-réseaux.

Un bon plan d'adressage IP peut donc offrir certains des avantages de la segmentation physique en limitant le travail d'administration du réseau ; il n'offre évidemment pas la même sécurité, mais assure un minimum de confort. Pour le réseau pédagogique d'un grand établissement scolaire, ce minimum paraît suffisant et contribue à une bonne gestion, à une bonne utilisation sans limiter les possibilités offertes aux utilisateurs.

Eléments de calcul - définitions et règles

Repérage

Une machine est repérée sur le réseau par une **adresse IP** (**IPx**) associée à un **masque** (**Mx**) qui sont chacun un nombre binaire de 3 bits organisé en 4 octets. Le masque sert à repérer le réseau ou le sous-réseau auquel la machine appartient. Ces deux nombres sont en général donnés en décimal, ce qui nous oblige à effectuer quelques petits calculs et conversions.
exemple 1 : IP1 = 192.168.20.34 et M1 = 255.255.255.0 se traduit en binaire par
IP1 = (1100 000).(1010 1000).(0001 0100).(0010 0010) et M1 = (1111 1111).(1111 1111).(1111 1111).(0000 000)
cette machine se repère en notation par 192.168.20.34 / 24 car le masque comporte 24 bits à 1.
exemple 2 : IP2 = 172.16.1.220 et M2 = 255.255.0.0 se traduit en binaire par
IP2 = (1010 1100).(0001 0000).(000 0001).(1101 1100) et M2 = (1111 1111).(1111 1111).(0000 000).(0000 000)
cette machine se repère en notation par 172.16.1.220 / 16 car le masque comporte 16 bits à 1.
note 1 : pour chaque octet : les 4 bits de gauche sont dits de poids fort et les 4 de droite de poids faible ; de même pour un nombre IP, les 2 octets de droite sont de poids fort et les 2 de gauche de poids faible.

Identification du réseau

Pour connaître un **numéro de réseau** (**R**) ou de **sous-réseau** (**Rx**), il faut poser l'opération logique : **R = (IP) AND (M)** , AND étant l'opérateur logique "ET" (cette opération se décompose en 32

opérations entre bits de même rang).
Dans l'exemple 1, cela donne : R1 = 192.168.20.0 qui se résume par 192.168.20 /24 ;
dans l'exemple 2, cela donne : R2 = 172.16.0.0 qui se résume par 172.16 / 16 ;
exemple 3 : soit une machine repérée par l'adresse **IP3 = 192.154.88.133 / 26** ;
on trouve son masque de sous-réseau en constatant que 26 = 8 + 8 + 8 + 2 ,
donc **M3 = 255.255.255.192** [en fait (1111 1111).(1111 1111).(11111111).(1100 0000)] ;
on en déduit le numéro du sous-réseau auquel elle appartient par l'opération (IP3) AND (M3), soit :
(1100 0000).(1001 1010).(0101 1000).(1000 0101)
(1111 1111).(1111 1111).(11111111).(1100 0000)
(1100 0000).(1001 1010).(0101 1000).(1000 0000) = **R3 = 192.154.88.128** .

Diffusion et nombre d'hôtes

L'**adresse** de **diffusion** (**Bx**) d'un réseau ou d'un sous-réseau est une adresse réservée (la dernière des adresses possibles du dit réseau). Cette adresse est utilisée pour transmettre des informations (paquets) à tous les hôtes du sous-réseau (plus exactement du domaine de diffusion) en même temps. Un paquet destiné à l'adresse Bx est forcément transmis à toutes les machines de Rx. Les commutateurs diffusent aussi les *broadcast*-s ; quand un de leurs ports reçoit une trame (suite de paquets) pour Bx, il la diffuse sur tous les autres ports. Seuls les routeurs (et a fortiori la segmentation physique) bloquent les *broadcast*-s.
Connaissant Mx et Rx, on trouve Bx par un petit calcul en décimal ; on opère octet par octet, en considérant chacun des octets de Rx, et en y ajoutant la différence entre 255 et la valeur de l'octet correspondant de Mx.
On trouve : B1 = 192.168.20.255 car R1 = 192.168.20.0 et M1 = 255.255.255.0 ;
on trouve : B2 = 172.16.255.255 car R2 = 172.16.0.0 et M1 = 255.255.0.0 ;
on trouve B3 = 192.154.88.191 car R3 = 192.154.88.128 et M3 = 255.255.255.192 .

La capacité maximale du réseau ou du sous-réseau, appelée le **nombre** d'**hôtes** (**Hx**), s'obtient aisément par le nombre **n** de bits à 1 du masque Mx : Hx = $\left[2^{(32-n)}-2\right]$; 2 adresses en moins car une est réservée pour l'adresse du sous-réseau lui-même et l'autre pour la diffusion du sous-réseau ("*broadcast*").
Dans l'exemple 1, H1 = 254 ; dans l'exemple 2, H2 = 65 534 et dans l'exemple 3, H3 = 62 .

Plus Hx est grand et plus la bande passante du réseau s'amenuise et le traffic de diffusion augmente.

A partir d'une adresse IP complète (ou CIDR), on peut obtenir tous les renseignements précédemment définis

adresse CIDR	Masque décimal	Numéro de réseau	Adresse de diffusion	nombre d'hôtes	étendue du (sous-) réseau
192.168.20.34 / 24	255.255.255.0	192.168.20.0	192.168.20.255	254	de 192.168.20.1 à 192.168.20.254
172.16.1.22	255.255.0.0	172.16.0.0	172.16.255.	65	de

0 / 16			255	534	172.16.0.1 à 172.16.255.254
192.154.88.133 / 26	255.255.255.192	192.154.88.128	192.154.88.191	62	de 192.154.88.129 à 192.154.88.190
131.108.78.235 / 21	255.255.248.0	131.108.72.0	131.108.79.255	2046	de 131.108.72.1 à 131.108.79.254

HAUT DU FORMULAIRE

Outil de calcul permettant d'ajuster le masque de sous-réseau

Entrer une adresse IP (*xxx.yyy.zzz.ttt)* et un masque (*mm*), l'outil renvoie :
la valeur du masque (*en décimal*), le nombre maximal d'hôtes, l'adresse du réseau, la 1ère et la dernière adresse utilisable.

adresse ip :

masque :

Visibilité des machines entre elles

Deux machines quelconques ayant le même numéro de sous-réseau (appartenant donc au même sous-réseau) peuvent mutuellement se voir - **attention il peut y avoir des contre-exemples** si les masques ne sont pas correctement organisés -.

Donnons ici une règle exacte.
Soient les machines A et B, repérées respectivement par (IPA - MA) et (IPB - MB) ;
A peut voir B si (IPA) AND (MA) = (IPB) AND (MA), ou encore si RA = (MA) AND (IPB) ;
B peut voir A si (IPB) AND (MB) = (IPA) AND (MB), ou encore si RB = (MB) AND (IPA) .

exemple 4 : soient la machine A [IPA = 192.168.1.80 / 26] et la machine B [IPB = 192.168.1.133 / 27] ;
on peut établir les caractéristiques suivantes :

adresse CIDR	Masque décimal	Numéro de réseau	Adresse de diffusion	nombre d'hôtes	étendue du (sous-) réseau
192.168.1.80 / 26	255.255.255.192	192.168.1.64	192.168.1.127	62	de 192.168.1.65 à 192.168.1.126
192.168.1.133 / 27	255.255.255.224	192.168.1.128	192.168.1.159	30	de 192.168.1.129 à 192.168.1.158

On constate que ces deux réseaux ont bien des numéros de réseau différents ; ils sont bien disjoints et même contigus.
(MA) AND (IPB) donne 192.168.1.128 , différent de RA ; A ne voit pas B ;

(MB) AND (IPA) donne 192.168.1.64 , différent de RB ; B ne voit pas A .

- Il faut s'assurer que les sous-réseaux sont bien disjoints et bien imbriqués.

- Ry est un sous-réseau de Rx si Ry est supérieur à Rx ; ainsi le réseau 172.20.10.0 est un sous-réseau du réseau 172.20.0.0 . Pratiquement, un serveur se trouve dans un réseau au moins plus large (Rx plus petit et donc Hx plus grand) que celui du client.

Passerelle ("*gateway*") : c'est un dispositif (routeur, modem, machine à 2 cartes) qui permet à une machine d'un réseau ou d'un sous-réseau de communiquer avec un réseau plus large ou avec un autre réseau. Pour remplir correctement sa fonction, le dispositif passerelle doit être vu par la machine voulant l'utiliser, et réciproquement. Une passerelle est une sorte d'aiguillage (parfois à plusieurs voies) qui permet la communication entre deux réseaux tout en limitant le trafic de diffusion.

Adressage automatique

Les machines d'un réseau peuvent obtenir dynamiquement une adresse IP depuis un dispositif (serveur ou routeur) se trouvant dans leur réseau. Ce type d'adressage s'oppose à l'adressage statique qui est paramétré 'à la main' sur chaque machine. L'adressage automatique est assuré par qui est un sous-protocole de IP.
DHCP est de plus en plus utilisé sur les petits réseaux d'autant plus qu'il permet de réserver une (ou plusieurs) plage précise d'adresses pour les machines qui se connectent au serveur DHCP, et que certaines machines, reconnues par leur adresse MAC, peuvent être octroyées d'une adresse unique.
Pour un grand réseau avec un seul serveur, DHCP devient réellement problématique puisque l'adresse attribuée par le serveur s'apparie d'un **masque identique à celui du serveur** ; toutes les machines vont donc se retrouver dans le même réseau avec les problèmes de bande passante et de diffusion que cela pose. Une solution est de segmenter le grand réseau en laissant le serveur DHCP dans le segment par défaut ("*default VLAN*"). Une autre est d'utiliser les sous-réseaux IP limités par un routeur passerelle offrant la fonctionnalité DHCP.

Dans tous les cas, l'utilisation de DHCP ne dispense pas l'administrateur d'une réflexion et d'un calcul préalable.

Une étude très fine doit être entreprise avant de mettre en oeuvre l'adressage des machines d'un grand réseau. Toutes les perspectives d'évolution doivent être envisagées et le cahier des charges (prise en compte de l'utilisation effective qui sera faite du réseau) doit être clair. Lorsque l'on veut limiter la diffusion, les contraintes sont plus importantes et les calculs doivent être scrupuleusement étudiés.